noSpamProxy® SERVER

Version 14

Integration von NoSpamProxy

- in Office 365
- in Microsoft Azure
- als On-Premises-Lösung

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

DIESES DOKUMENT WURDE ZULETZT AM 27. NOVEMBER 2023 ÜBERARBEITET.

Inhalt

Einleitung

Seit Version 10 ist NoSpamProxy® vollständig in Microsoft 365 integrierbar. Dieses Handbuch beschreibt die Konfigurationsschritte sowohl für NoSpamProxy und Microsoft 365 als auch für die eingesetzte Serverumgebung.

Die beschriebene Konfiguration gilt dabei ebenso für den Einsatz von NoSpamProxy als On-Premises-Lösung und in Microsoft Azure.

HINWEIS: Die spezifischen Konfigurationsschritte für den Einsatz in Microsoft Azure werden unter **Notwendige Konfigurationen für den Betrieb in Microsoft Azure** beschrieben.

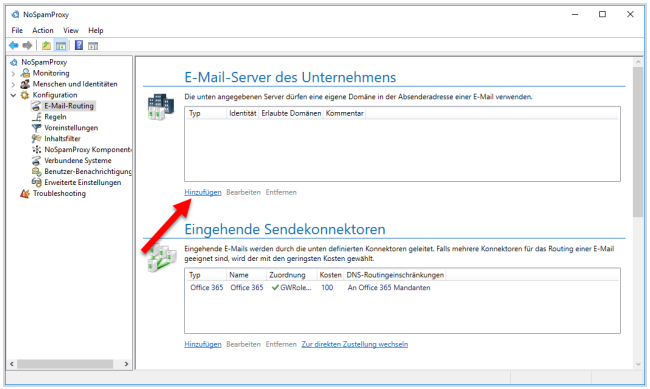
Microsoft 365 als Relayhost freigeben

In diesem Schritt lassen Sie Microsoft 365 in der NoSpamProxy®-Konfiguration als Relayhost zu, damit E-Mails aus Microsoft 365 heraus durch NoSpamProxy an externe Kommunikationspartner verschickt werden können.

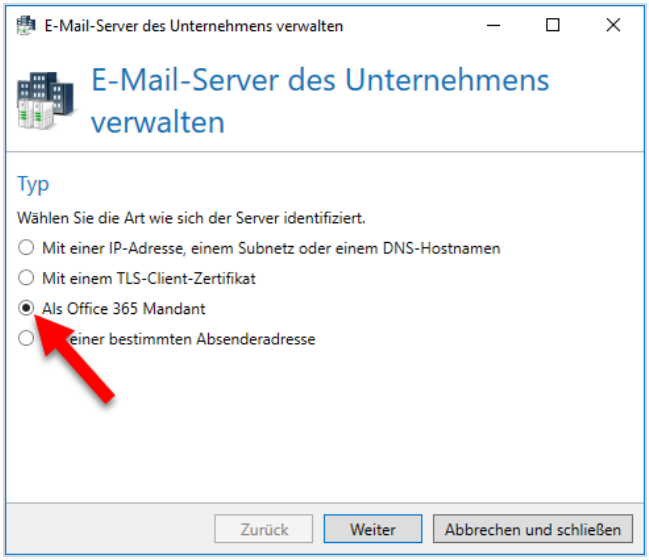
Ohne diese Konfiguration wird NoSpamProxy E-Mails als Relay-Missbrauchsversuch bewerten und abweisen.

> **HINWEIS:** Stellen Sie sicher, dass Sie mindestens eine Unternehmensdomäne eingerichtet haben, bevor Sie mit der Konfiguration beginnen.

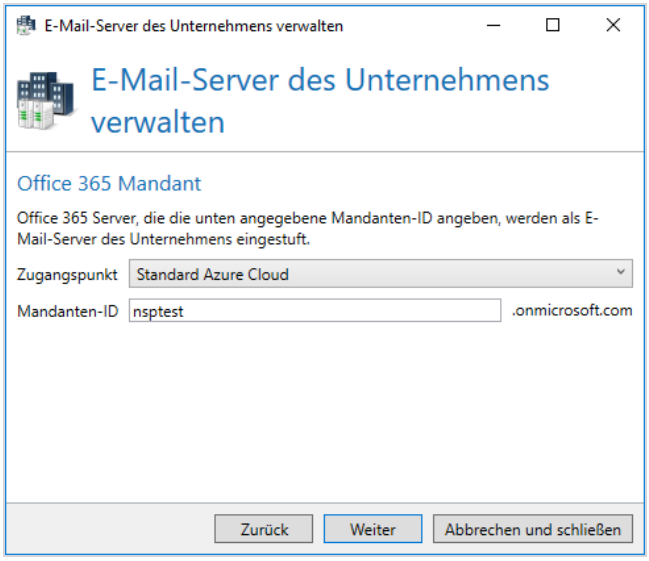
1. Wechseln Sie im NoSpamProxy Command Center zu **Konfiguration > E-Mail-Routing** und klicken Sie **Hinzufügen**.



2. Wählen Sie den Typ **Als Office 365 Mandant** und klicken Sie danach **Weiter**.



3. Treffen Sie unter **Zugangspunkt** die für Ihre Organisationsumgebung passende Auswahl.
4. Geben Sie ihre Mandanten-ID ein. Achten Sie darauf, dass Sie den Namen der ID eingeben (nicht die ID in hexadezimaler Schreibweise).
5. Klicken Sie **Weiter**.



6. Wählen Sie unter **Zugeordnete Unternehmensdomänen** die Domänen aus, die Sie in Microsoft 365 hinterlegt haben und die in der Absenderadresse für ausgehende E-Mails vorkommen werden.

   > **HINWEIS:** Wenn Sie hier nicht alle Domänen vorfinden, müssen Sie die fehlenden Domänen unter **Identitäten > Unternehmensdomänen > Unternehmensdomänen** hinzufügen. Dies ist auch zu einem späteren Zeitpunkt möglich.

7. Klicken Sie **Weiter**.
8. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie dann **Fertigstellen**.

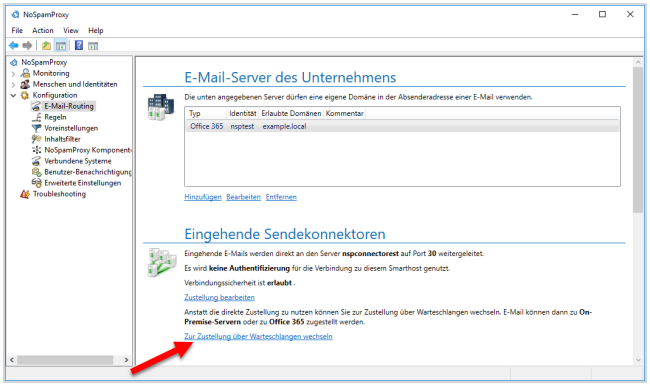
Der E-Mail-Server ist nun angelegt.

Weiterleitung an Microsoft 365 einrichten

> **HINWEIS:** Für die Einrichtung der Weiterleitung an Microsoft 365 ist ein TLS-Zertifikat erforderlich, dass von einer von Microsoft vertrauten Stammzertifizierungsstelle ausgestellt wurde. Eine aktuelle Liste der vertrauten Stellen finden Sie unter **https://docs.microsoft.com/en-us/security/trusted-root/participants-list**.

In diesem Schritt konfigurieren Sie NoSpamProxy® so, dass alle eingehenden E-Mails an Microsoft 365 weitergeleitet werden. Dazu müssen Sie die entsprechenden Sendekonnektoren bearbeiten.

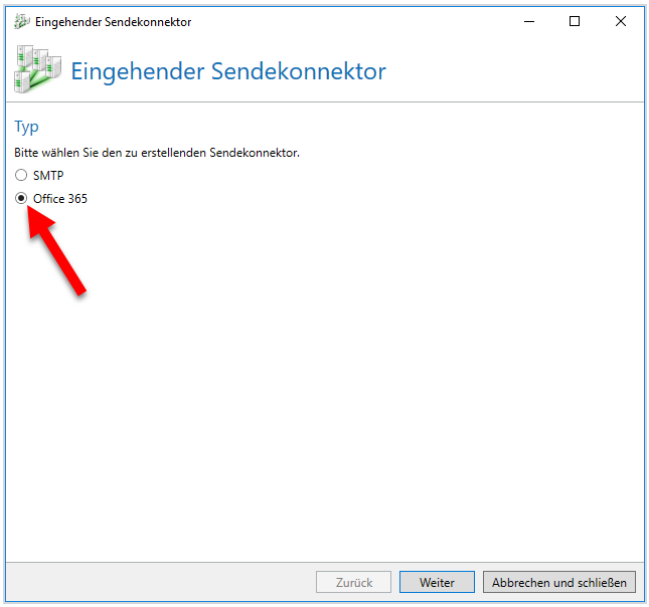
1. Wechseln Sie zu **Konfiguration > E-Mail-Routing**.
2. Klicken Sie unter **Eingehende Sendekonnektoren** auf **Zur Zustellung über Warteschlangen wechseln**.



3. Wählen Sie im Dialog **Zustellung ändern** die Option **Zustellung ersetzen**.

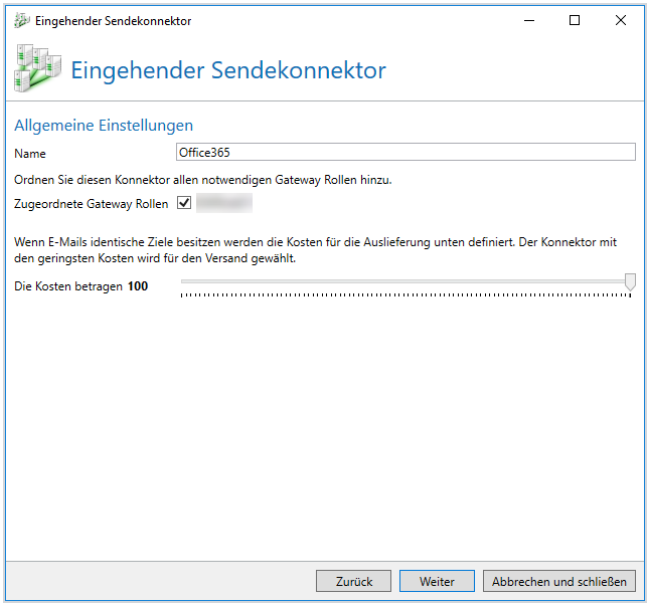
> **HINWEIS:** Ab Version 13 entfällt dieser Schritt, da die direkte Zustellung ab dieser Version nicht mehr unterstützt wird.

4. Wählen Sie im dann folgenden Dialog **Office 365** und klicken Sie **Weiter**.

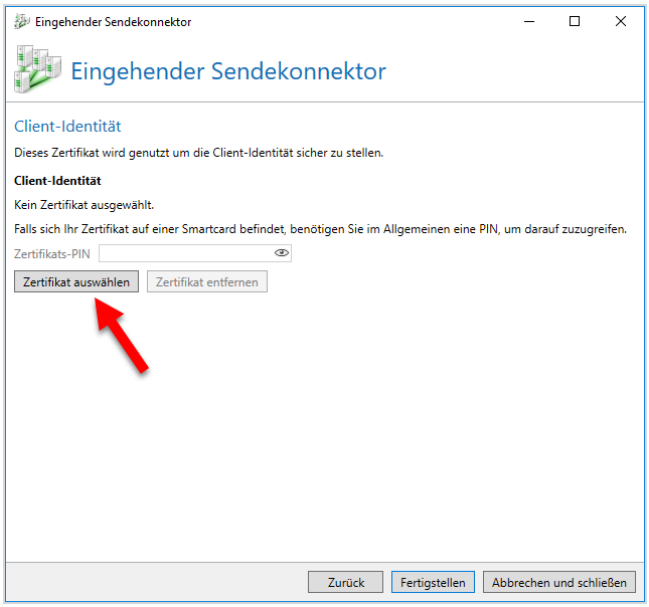


5. Geben Sie einen beliebigen Namen für den eingehenden Sendekonnektor ein und wählen Sie danach die Gatewayrolle(n) aus, die E-Mails an Office 365 verarbeiten sollen.

6. Klicken Sie **Weiter**.



7. Klicken Sie **Zertifikat auswählen**, um ein Zertifikat für die Client-Identität anzugeben, mit dem sich NoSpamProxy beim Office-365-Server authentifizieren kann.



8. Wählen Sie im dann folgenden Dialog das TLS-Zertifikat aus, das Sie zuvor bei einer von Microsoft vertrauten Stammzertifizierungsstelle beantragt haben und klicken Sie danach **Auswählen und schließen**.
9. Klicken Sie **Auswählen und schließen**.
10. Klicken Sie im folgenden Dialogfenster **Fertigstellen**.
11. Öffnen Sie unter **Empfangskonnektoren** den genutzten Empfangskonnektor und wechseln Sie zur Registerkarte **Verbindungssicherheit**.
12. Wählen Sie entweder das von NoSpamProxy mitgelieferte oder das zuvor beantragte Zertifikat aus.
13. Klicken Sie **Auswählen und schließen** und dann **Speichern und schließen**.

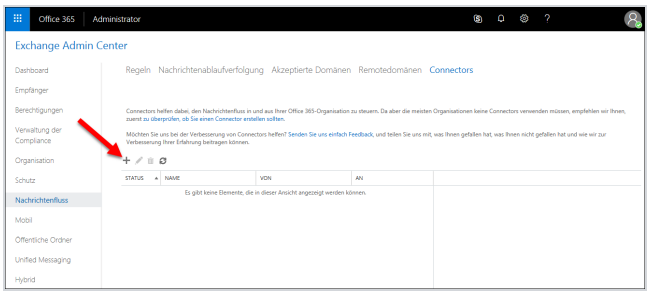
Die Konfiguration für NoSpamProxy ist nun abgeschlossen.

Microsoft 365 konfigurieren

In diesem Schritt konfigurieren Sie den Office-365-Mandanten so, dass ausgehende E-Mails nicht direkt an den Empfängerserver, sondern zunächst an NoSpamProxy® zugestellt werden. Melden Sie sich dazu in an Ihrem Office-365-Mandanten unter **https://outlook.office365.com/ecp** an.

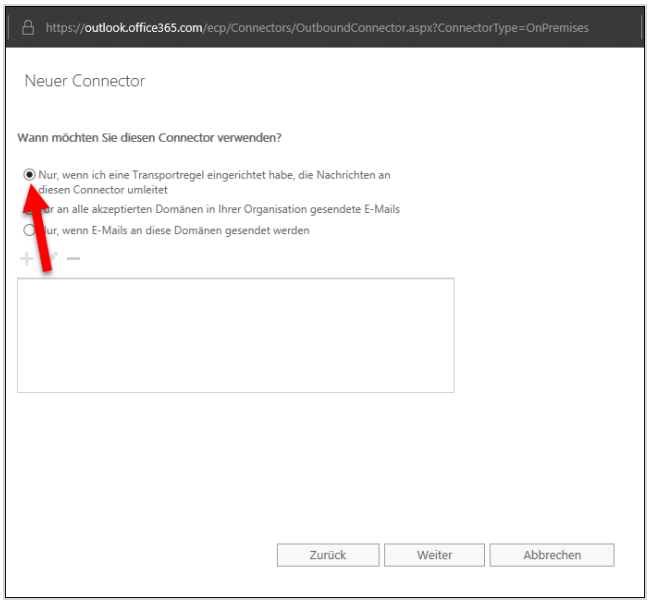
> **HINWEIS:** Verwenden Sie für die Anmeldung einen Benutzer, der über Administrationsrechte verfügt.

1. Wechseln Sie im Exchange Admin Center zu **Nachrichtenfluss > Connectors**; klicken Sie danach das **Plus-Zeichen**. Der Assistent zum Anlegen eines neuen Connectors öffnet sich.

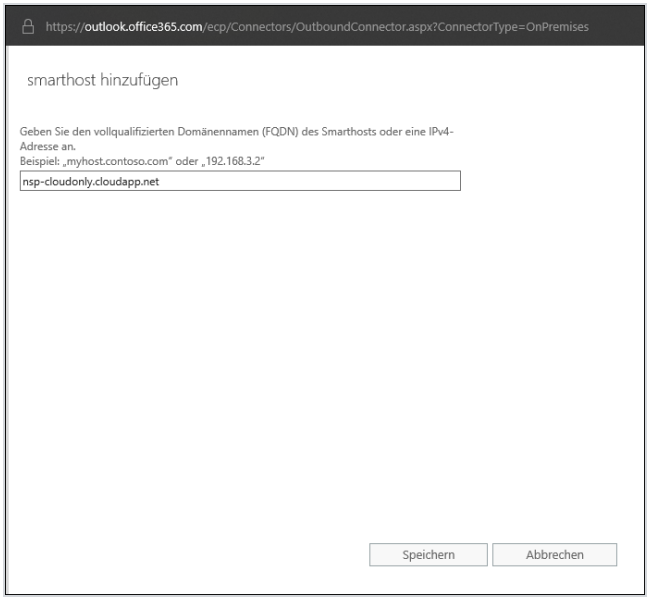


2. Wählen Sie auf der ersten Seite im Feld **Von** die Option **Office 365** aus; wählen Sie im Feld **An** die Option **Partnerorganisation** aus.
3. Klicken Sie **Weiter**. Mit dieser Einstellung werden ausgehende E-Mails vom Office-365-Mandanten an NoSpamProxy gesendet.
4. Geben Sie auf der dann folgenden Seite einen beliebigen Namen für den Connector ein.
5. Geben Sie bei Bedarf eine Beschreibung ein und klicken Sie **Weiter**.

6. Wählen Sie auf der dann folgenden Seite die Option **Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Konnektor umleitet**.
7. Klicken Sie **Weiter**.

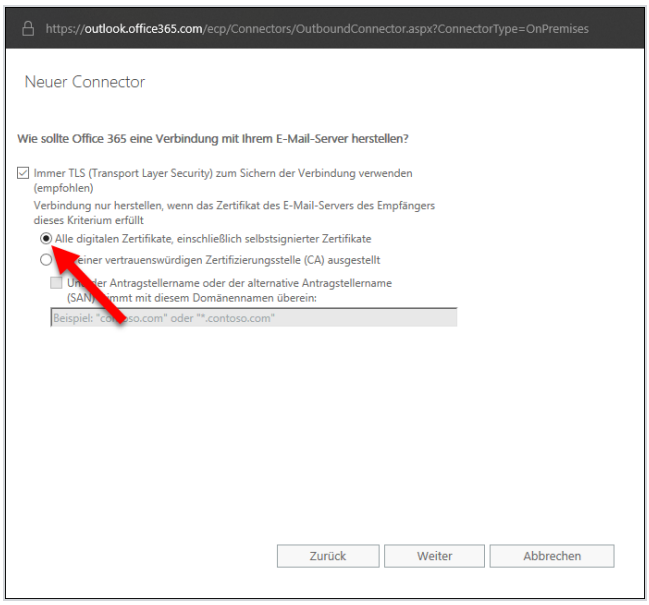


8. Geben Sie den Namen oder die IP-Adresse des Servers (Smarthost) an, auf dem die Gatewayrolle installiert ist und klicken Sie danach **Speichern**.



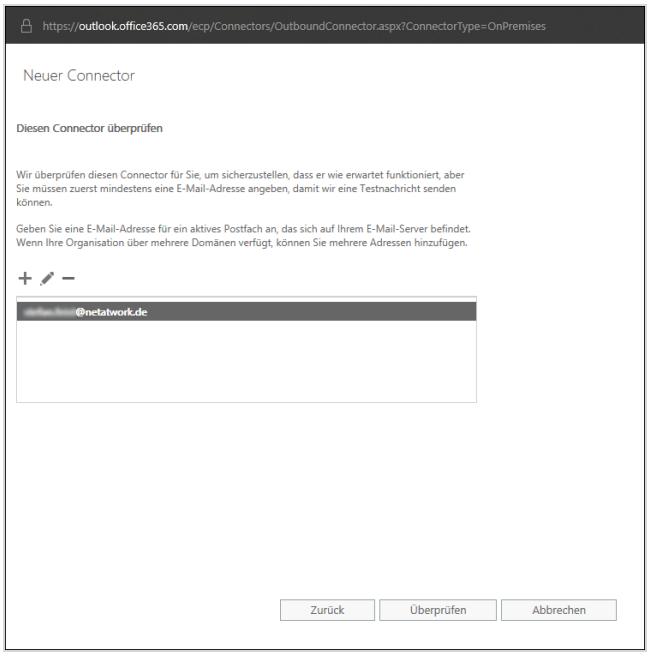
> **HINWEIS:** Beachten Sie beim Eintragen des Hostnamens, dass Microsoft 365 bei der Auflösung die MX-Einträge vor den A-Einträgen betrachtet. Sollte für den eingetragenen Hostnamen neben einem A-Eintrag auch ein MX-Eintrag existieren, wird der Konnektor auf diesen zurückgreifen.

9. Aktivieren Sie im folgenden Dialogfenster die Option **Immer TLS zum Sichern der Verbindung verwenden**. Im darunterliegenden Dialogfenster wählen Sie den Punkt **Alle digitalen Zertifikate, einschließlich selbstsignierter Zertifikate** aus und klicken **Weiter**.



10. Kontrollieren Sie die Zusammenfassung Ihrer Angaben auf Richtigkeit und klicken Sie **Weiter**.

11. Geben Sie im folgenden Dialog eine oder mehrere E-Mail-Adressen ein, die Sie für die Überprüfung dieses Konnektors verwenden möchten.



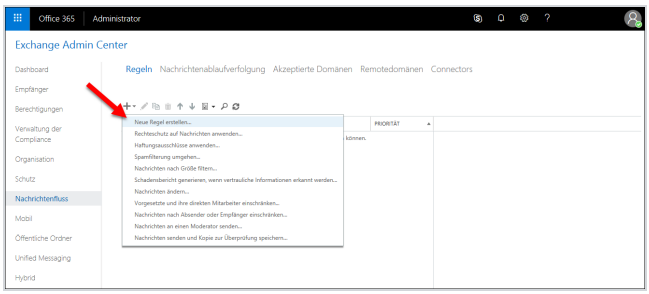
12. Klicken Sie **Überprüfen**.

> **HINWEIS:** Es werden nun eine oder mehrere Test-Nachrichten gesendet. Nach Abschluss der Prüfung erhalten Sie ein Überprüfungsergebnis. Die Test-Nachricht schlägt in der Regel fehl; dies können Sie zunächst ignorieren.

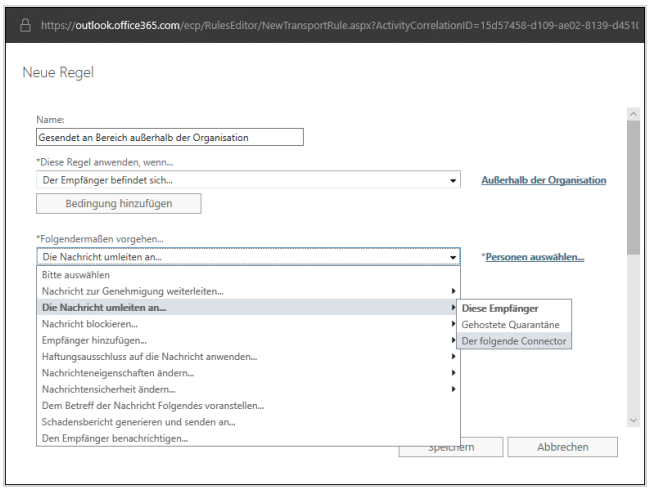
13. Klicken Sie **Speichern**, um den Dialog zu schließen.

Die Transportregel erstellen

1. Gehen Sie in der Office-365-Verwaltungsoberfläche zu **Nachrichtenfluss > Regeln**.
2. Klicken Sie das **Plus-Symbol**.



3. Wählen Sie danach die Option **Neue Regel erstellen**. Der Assistent für die Erstellung einer neuer Transportregel öffnet sich.



4. Geben Sie einen beliebigen Namen für die Regel ein.
5. Stellen Sie unter **Diese Regel anwenden wenn** die folgenden Optionen ein:
    - **Der Empfänger befindet sich** sowie
    - **Außerhalb der Organisation**.

6. Stellen Sie unter **Folgendermaßen vorgehen** die Option **Folgenden Connector verwenden** ein.
7. Geben Sie danach den vorher erstellten Konnektor an und klicken Sie **OK**.

> **HINWEIS:** Falls Sie an dieser Stelle nur **Personen** auswählen können, klicken Sie im unteren Abschnitt **Weitere Optionen**. Dort können Sie unter **Die Nachricht umleiten an** die Option **Folgenden Connector verwenden** auswählen. Anschließend können Sie den zuvor erstellten Konnektor verwenden.

8. Klicken Sie **Speichern**.

Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online

Wenn Sie NoSpamProxy® in Microsoft 365 in Verbindung mit Exchange Online nutzen, müssen Sie in Ihrem Tenant zusätzliche Einstellungen vornehmen, die die Spamabwehr sicherstellen.

Schritt 1: Anlegen eines eingehenden Connectors für die Domain *

Um die Zustellung von unerwünschten E-Mails aus dem Internet zu unterbinden, legen Sie einen eingehenden Connector an. Dieser Connector erlaubt für die Domain * nur E-Mails von bestimmten IP-Adressen - Ihrem eigenen E-Mail-Server oder NoSpamProxy. Hierfür wird ein entsprechender Partner Connector benötigt.

Um den Partner Connector in PowerShell anzulegen, geben Sie Folgendes ein:

```
New-InboundConnector

-Name "NurE-MailsVonDiesemServerAkzeptieren<NoSpamProxy>"

-ConnectorType Partner

-SenderDomains *
```

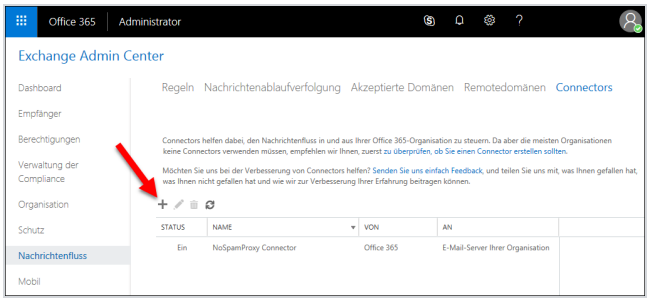
```
-RestrictDomainsToCertificate $true

-TlsSenderCertificateName <DasZuvorErstellteUndAusgewählteZertifikat>

-AssociatedAcceptedDomains

<AlleDomänenDieInNoSpamProxyUnterEigeneDomänenStehenUndImOffice365TenantVerwendetWerden>
```

WARNUNG: Um den Spam-Schutz durch NoSpamProxy® sicherzustellen, müssen Sie sämtlichen eingehenden E-Mail-Verkehr über NoSpamProxy leiten und Microsoft 365 ausschließlich durch NoSpamProxy unter Verwendung eines dedizierten Konnektors ansprechen. Ansonsten ist es möglich, dass sich die Anti-Spam-Funktionalitäten von NoSpamProxy und Exchange Online Protection (EOP) gegenseitig behindern. Wir empfehlen Ihnen dringend, diese Einstellung vorzunehmen, da die Sicherheit und Stabilität Ihrer Konfiguration sonst nicht gewährleistet ist.

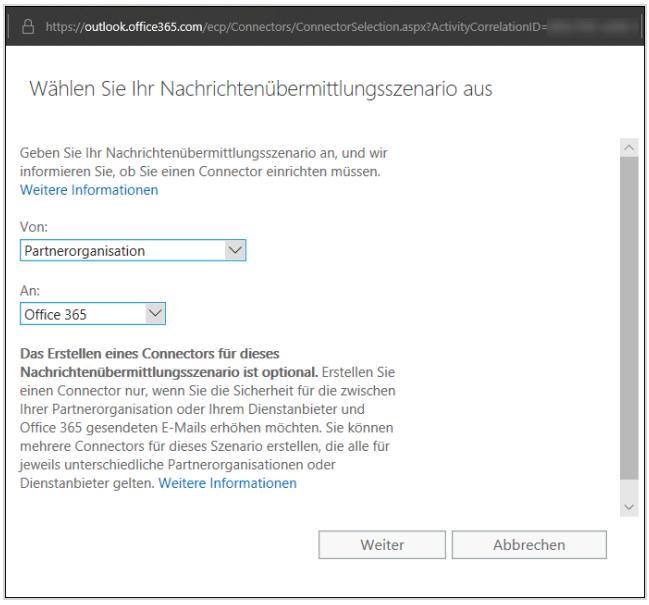
TIPP: Sie können an Stelle der IP-Adresse auch das Zertifikat des einliefernden Gateways hinterlegen.

Um den Partner Connector über das Exchange Control Panel anzulegen, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Nachrichtenfluss > Connectors** und klicken Sie das **Plus-Zeichen**.

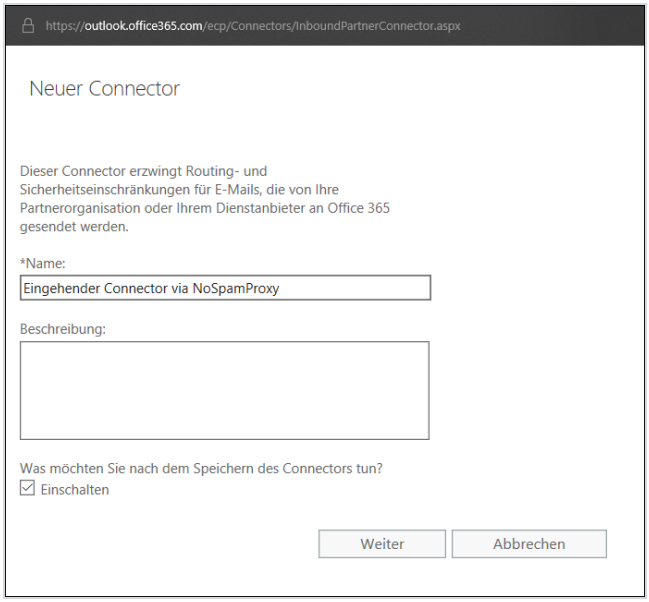


2. Wählen Sie im Dialogfenster die Optionen **Partnerorganisation** und **Office 365** aus und klicken Sie danach **Weiter**.

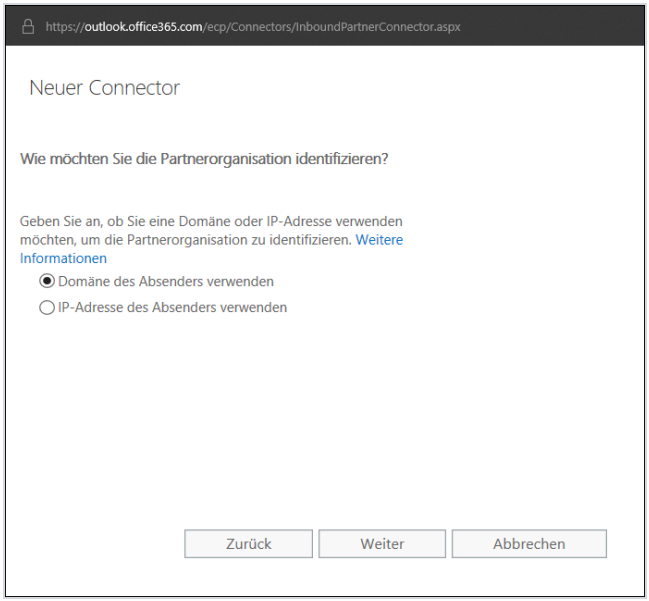


3. Geben Sie im Dialog **Neuer Connector** einen Namen für den Connector ein und fügen Sie bei Bedarf eine Beschreibung hinzu. Lassen Sie das Häkchen

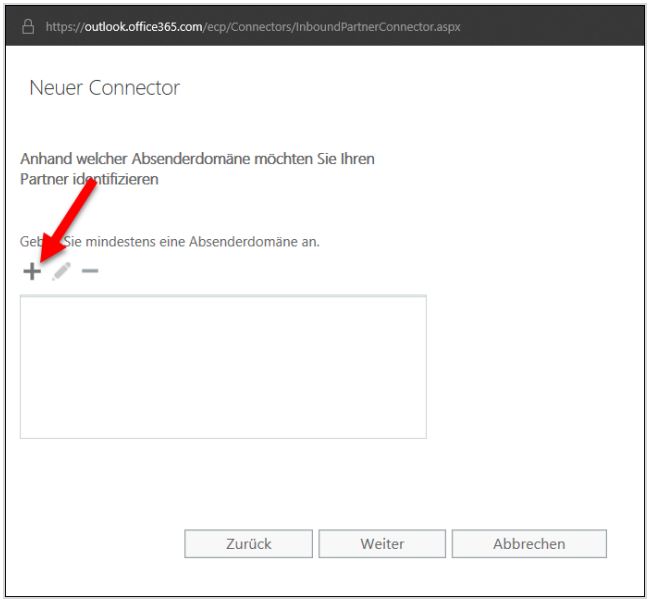
neben **Einschalten** gesetzt. Klicken Sie dann **Weiter**.



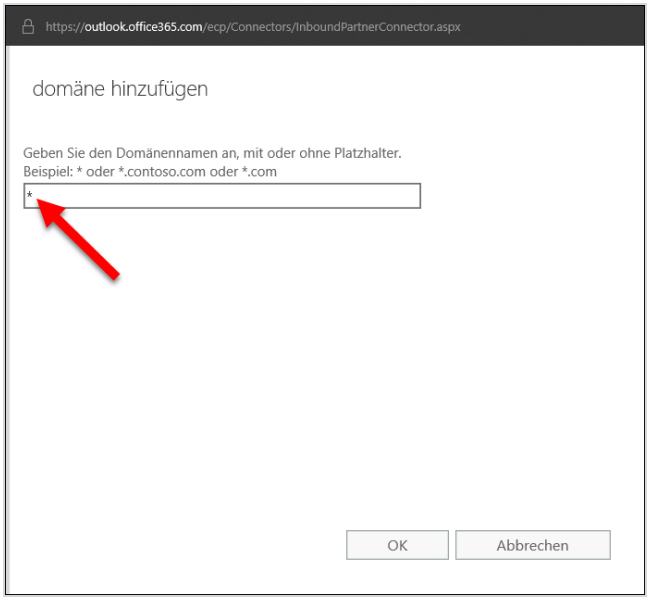
4. Wählen Sie im folgenden Dialogfenster die Option **Domäne des Absenders** und klicken Sie danach **Weiter**.



5. Klicken Sie im folgenden Dialogfenster das **Plus-Zeichen**.

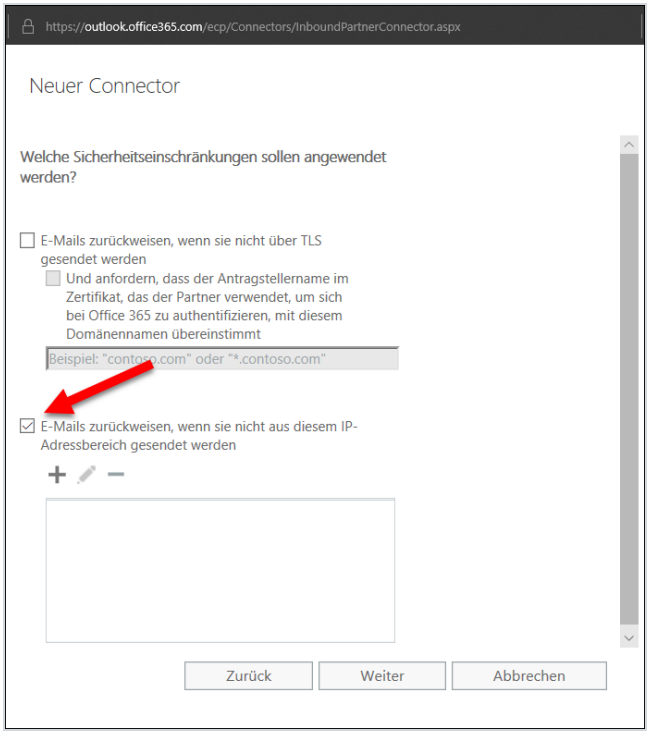


6. Geben Sie als Domainnamen ein Sternchen ("*") ein. Klicken Sie danach **OK** und auf der folgenden Seite **Weiter**.

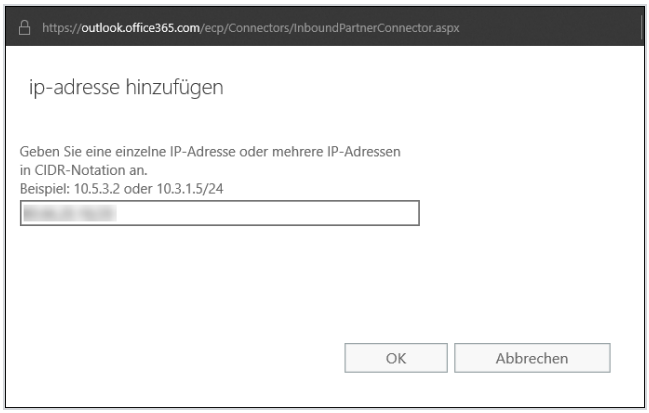


7. Setzen Sie auf der folgenden Seite das Häkchen bei **E-Mails zurückweisen, wenn Sie nicht aus diesem Adressbereich gesendet werden**. Klicken Sie

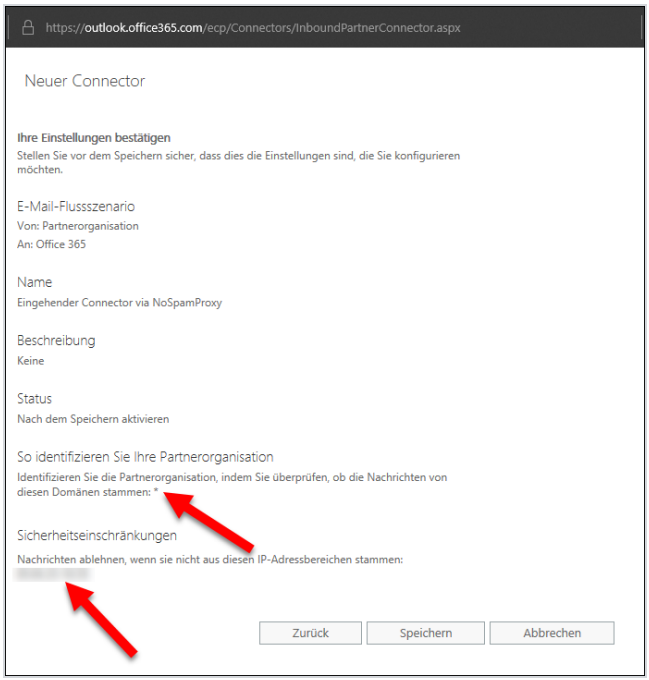
Weiter.



8. Geben Sie im Dialog **IP-Adresse hinzufügen** die Adresse des Servers an, auf dem die Gatewayrolle installiert ist. Klicken Sie **OK**.



9. Überprüfen Sie die Angaben in der Zusammenfassung auf Richtigkeit und klicken Sie **OK**.

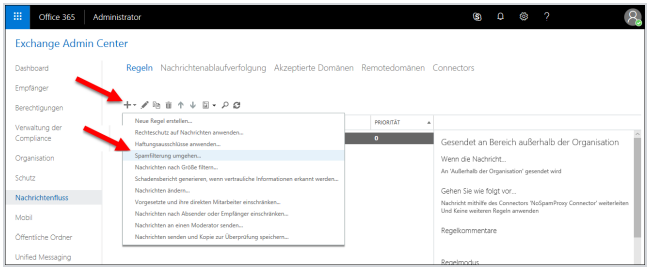


Der neue Connector erscheint jetzt unter **Nachrichtenfluss/Connectors**.

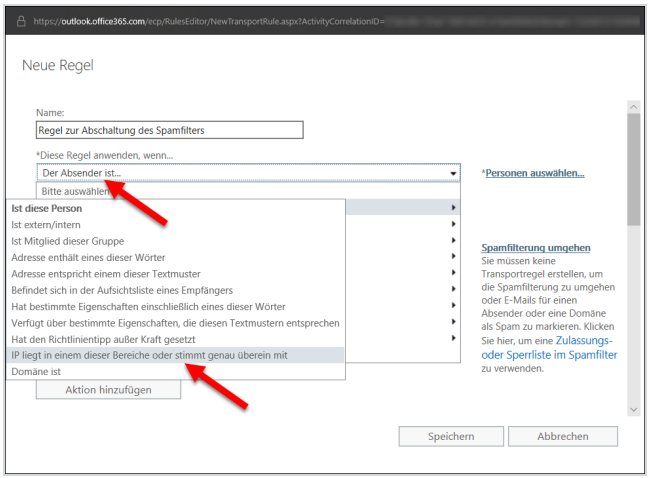
Schritt 2: Anlegen einer Transportregel zur Abschaltung des Spamfilters

1. Gehen Sie zu **Nachrichtenfluss/Regeln**.
2. Klicken Sie das **Plus-Zeichen**.
3. Wählen Sie **Spamfilterung umgehen** aus dem Drop-Down-Menü.

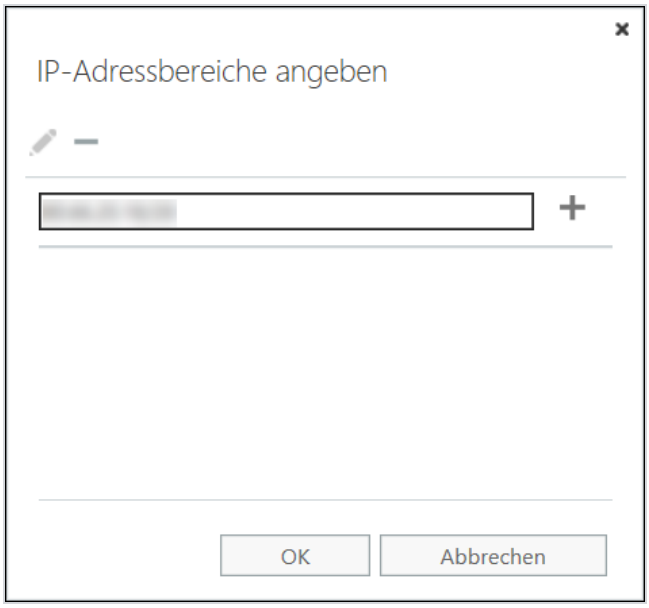
4. Geben Sie der Regel einen Namen.



5. Wählen Sie unter **Diese Regel anwenden, wenn** die Option **Absender** und danach **IP liegt in einem dieser Bereiche oder stimmt genau überein mit**.



6. Geben Sie im Dialog **IP-Adressbereiche angeben** die IP-Adresse des Servers an, auf dem die Gatewayrolle installiert ist.



7. Klicken Sie das **Plus-Zeichen** und danach **OK**.
8. Klicken Sie **Speichern**.

Die Regel ist nun eingerichtet. Der Spamschutz für die Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online ist sichergestellt.

Notwendige Konfigurationen für den Betrieb in Microsoft Azure

Einbinden des TCP Proxy

> **HINWEIS:** Sie müssen über einen gültigen Vertrag über Softwarewartung verfügen, um den TCP Proxy nutzen zu können.

Bei einigen cloudbasierten Systemen – zum Beispiel in Microsoft Azure – kann es vorkommen, dass der Port 25 ausgehend vom Anbieter blockiert wird. Port 25 wird aber zum Versand von E-Mails benötigt, was einen Betrieb von NoSpamProxy auf einem solchen System behindert.

Hierzu bieten wir eine Alternative an, um solche Systeme trotzdem zu nutzen: unseren *TCP Proxy*. Dieses System kann auf unten beschriebene Weise in NoSpamProxy aktiviert werden. Dabei wird jede ausgehende Verbindung an eine routing-fähige IPv4-Adresse auf TCP-Ebene durch den TCP Proxy für NoSpamProxy geroutet. Die E-Mails werden dann vom Server aus über Port 443 an den TCP Proxy gesendet und von dort dann über Port 25 weiter zum Empfängersystem geleitet.

1. Stoppen Sie den Dienst der Gatewayrolle über das NoSpamProxy Command Center oder die Windows-Dienste
2. Öffnen Sie als Administrator einen Texteditor auf dem System, auf dem die Gatewayrolle installiert ist.
3. Öffnen Sie die Konfigurationsdatei **Gateway Role.config** aus dem Verzeichnis **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

4. Suchen Sie in der Datei nach `<smtpServicePointConfiguration>` und ändern/fügen Sie den Wert

```
isProxyTunnelEnabled="true"
proxyTunnelAddress="proxy.nospamproxy.com"
```

als Attribute hinzu. Falls `<smtpServicePointConfiguration` nicht vorhanden ist, suchen Sie nach `<netatwork.nospamproxy.proxyconfiguration` und fügen Sie

```
<smtpServicePointConfiguration
isProxyTunnelEnabled="true"
proxyTunnelAddress="proxy.nospamproxy.com" />
```

direkt unter diesem Wert hinzu.

5. Speichern Sie die Datei ab und schließen Sie den Editor.
6. Legen Sie das **Root CA Zertifikat** im Zertifikatsspeicher von Microsoft im Computerkonto unter **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** auf dem Server mit der Gatewayrolle ab.
7. Bearbeiten Sie im NoSpamProxy Command Center unter **Konfiguration > NoSpamProxy Komponenten > Gatewayrollen** die entsprechende Gatewayrolle und ändern Sie den Wert für **SMTP Servername** auf den Wert `outboundproxy.nospamproxy.com`.
8. Starten Sie den Gatewayrollen-Dienst wieder

9. Öffnen Sie die Datei **Gateway Role.config** erneut und prüfen Sie, ob der Wert beim Start erhalten geblieben ist.

Anpassen des SPF-Eintrags

- Wenn der TCP-Proxy implementiert ist, tritt dieser als absendendes System auf. Somit muss der TCP-Proxy auch mit in Ihrem SPF-Eintrag aufgenommen werden. Wir empfehlen dringend, folgenden Eintrag in Ihren SPF-Eintrag hinzuzufügen:

```
include:_spf.proxy.nospamproxy.com
```

Gegebenenfalls: Anpassen von Microsoft 365

Falls Sie aus Azure heraus E-Mails an eine eigene Microsoft-365-Instanz schicken, bei der ein Konnektor auf die IP-Adressen gebunden ist, aktualisieren Sie bitte die IP-Adressen passend zum Namen outboundproxy.nospamproxy.com. Da bei Microsoft 365 die TLS-Zertifikate gegen die HELO-Domain geprüft werden, ist es nur mit deutlich erhöhtem Aufwand möglich, dies entsprechend umzusetzen. Wir empfehlen daher eine Validierung anhand des Namens.

Gegebenenfalls: Anpassen der Firewall

- Falls Sie ausgehende Verbindungen gezielt blockieren, sollten Sie die Ausnahme für den TCP Proxy so anpassen, dass Verbindungen zum **IP-Netz 193.37.132.0/24** erlaubt sind.

Einrichten einer statischen IP-Adresse

Wenn Sie NoSpamProxy oder Teile davon in einer virtuellen Maschine in einer Microsoft-Azure-Umgebung betreiben möchten, benötigen Sie eine IP-Adresse, die auch nach dem Neustart der Maschine erhalten bleibt. Um dies zu erreichen, müssen Sie eine statische IP-Adresse (Reserved IP Address) einrichten. Ansonsten ist es möglich, dass nach dem Neustart der Maschine eine andere IP-Adresse zugewiesen wird.

HINWEIS: Diese Einstellung nehmen Sie auf dem virtuellen Computer in Microsoft Azure vor, auf dem NoSpamProxy installiert ist.

1. Öffnen Sie die Webseite **portal.azure.com**.
2. Klicken Sie unter **Home > Virtuelle Computer** auf den virtuellen Computer, auf dem NoSpamProxy installiert ist.
3. Gehen Sie zu **Netzwerk > Netzwerkschnittstelle > IP-Konfigurationen** und wählen Sie die für NoSpamProxy relevante Konfiguration.
4. Aktivieren Sie die Option **Öffentliche IP-Adresse** und klicken sie danach **Neu erstellen**.
5. Geben Sie einen Namen ein und wählen Sie die Option **Statisch** aus.
6. Klicken Sie **OK**.

Die IP-Adresse wird nun unter dem angegebenen Namen angezeigt.

> **HINWEIS:** Beachten Sie beim Einrichten einer statischen IP-Adresse die Informationen von der entsprechenden **Seite der Microsoft-Dokumentation**.

Anpassen des Reverse-DNS-Eintrags für den NoSpamProxy-Server

1. Öffnen Sie **portal.azure.com**.
2. Gehen Sie zu **Dashboard > Ressourcengruppen > [DieRessourcengruppeZuDerDerVirtuelleComputerGehoert] > [IhrVirtuellerComputer] > Eigenschaften**.
3. Geben Sie unter **DNS-Namensbezeichnung** einen Namen für die öffentliche IP-Adresse an.
4. Starten Sie die Azure Shell.
5. Geben Sie den folgenden Befehl ein und ersetzen Sie dabei die vorhandenen Platzhalter:

```
az network public-ip update --resource-group
[Ressourcengruppe] --name [NameDerIPAdresse] --
reverse-fqdn [VollstaendigerDNSName]  --dns-name
[DNSName]
```

HINWEIS: Beachten Sie auch die Anweisungen auf der entsprechenden **Seite der Microsoft-Azure-Dokumentation**.

Hilfe und Unterstützung

Knowledge Base

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

Website

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

Blog

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.

YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter **+49 5251304-636**
- per E-Mail unter **support@nospamproxy.de**.